JOURNAL OF COMBINATORIAL THEORY, Series A 25, 288–318 (1978)

Self-Dual Codes over *GF*(4)

F. J. MACWILLIAMS, A. M. ODLYZKO, AND N. J. A. SLOANE

Bell Laboratories, Murray Hill, New Jersey 07974

AND

H. N. WARD

University of Virginia, Charlottesville, Virginia 22901

Communicated by the Editors

Received December 6, 1976

This paper studies codes $\mathscr{C}$ over $GF(4)$ which have even weights and have the same weight distribution as the dual code $\mathscr{C}^\perp$. Some of the results are as follows. All such codes satisfy $\mathscr{C}^\perp = \bar{\mathscr{C}}$. (If $\mathscr{C}^\perp = \mathscr{C}$, $\mathscr{C}$ has a binary basis.) The number of such $\mathscr{C}$'s is determined, and those of length $\leqslant 14$ are completely classified. The weight enumerator of $\mathscr{C}$ is characterized and an upper bound obtained on the minimum distance. Necessary and sufficient conditions are given for $\mathscr{C}$ to be extended cyclic. Two new 5-designs are constructed. A generator matrix for $\mathscr{C}$ can be taken to have the form $[I \mid B]$, where $B^\perp = \bar{B}$. We enumerate and classify all circulant matrices B with this property. A number of open problems are listed.

1. INTRODUCTION

Background and motivation. Self-dual codes[1] are important for a number of practical and theoretical reasons [1, 6, 7, 9, 20–26, 28, 30, 32]. These codes are of greatest interest when the weights[1] of the code words are divisible by a constant. A theorem of Gleason, Pierce, and Turyn [3, 4, 36] says that, except for certain trivial codes with minimum distance 2, there are only three cases in which a self-dual or formally self-dual code over a field $GF(q)$ can have all weights divisible by a constant $c > 1$: namely $q = 2$ and $c = 2$ or 4, $q = 3$ and $c = 3$, and $q = 4$ and $c = 2$. The first two cases have been studied in several papers [10, 24–26, 28, 30, 35]. In the present paper we consider the remaining case $q = 4$, $c = 2$. There are some surprises (e.g., Theorems 4 and 6).

[1] These and other terms from coding theory are defined below.

0097-3165/78/0253–0288$02.00/0

Main results. An even code $\mathscr{C}$ must satisfy $\mathscr{C} \subseteq \mathscr{C}^{\perp}$ (Theorem 1), an even $[n, \frac{1}{2}n]$ code is formally self-dual (f.s.d.) (Theorem 4), and an even strictly self-dual code has a binary generator matrix (Theorem 6). An even f.s.d. code is monomially equivalent to one containing **1** (Corollary 9). The weight enumerator and complete weight enumerator of an even f.s.d. code are characterized (Theorems 13 and 17), and an upper bound on the minimum distance is given in Corollary 15 and Theorem 16. The parameters of the associated 5-designs (when they exist) are given explicitly (Theorem 18), and two new 5-designs are found (Eq. (18)). The numbers of even f.s.d. codes and even codes $\mathscr{C} \subseteq \mathscr{C}^{\perp}$ are given (Theorems 19 and 25).

The approximately 10^{16} even f.s.d. codes of length $\leqslant 14$ are classified: there are 19 inequivalent, indecomposable codes (Theorem 27). Several theorems for classifying those codes are given (Theorems 28–30). A uniformly packed code hypothesized by Bassalygo *et al.* [5] does not exist (Theorem 31).

Necessary and sufficient conditions are given for an even f.s.d. code of length $n + 1$ to be an extended cyclic code. If there is such a code, n is called feasible, and several characterizations of feasible numbers are found (Theorems 34–37). We also show how to find the idempotents of these cyclic codes (Section 5).

An even f.s.d. code can be constructed from a matrix B with $B\bar{B}^T = I$ (Theorem 5). In the last section we determine the number of circulant matrices of this type and show how to find them.

It is worth remarking that there is a code which plays the same role over $GF(4)$ as the binary and ternary Golay codes (cf. [21]). This is the [6, 3, 4] code E_6 of Table IV. In all three cases these are f.s.d. codes with gaps in their weight enumerators, the automorphism groups are larger than they need be, and the shortened codes are perfect quadratic-residue codes. E_6 is also a maximum distance separable Hamming code (cf. [21]).

In the same spirit we remark that there is a [24, 12, 8] binary code and a [24, 12, 9] ternary code [21], so it would be nice to decide whether the [24, 12, 10] $GF(4)$ code mentioned in Open Problem (2) exists. Several other open problems are also mentioned.

Finally, the paper contains several useful tables: extremal weight enumerators (Table I), the highest minimum distance of f.s.d. and self-dual codes (Table II), the number of even f.s.d. codes (Table III), all indecomposable even f.s.d. codes of length $\leqslant 14$ (Table V), and some even f.s.d. codes which are extended cyclic codes (Table VI).

Terminology. We take the elements of $GF(4)$ to be 0, 1, α, β with $\beta = \alpha^2 = \alpha + 1$, $\alpha^3 = \beta^3 = 1$. A *linear code* $\mathscr{C}$ *over* $GF(4)$ of *length* n and *dimension* k consists of 4^k vectors $\mathbf{u} = (u_1 \cdots u_n)$, $u_i \in GF(4)$, called *code words*, such that if $\mathbf{u}, \mathbf{v} \in \mathscr{C}$ then $\mathbf{u} + \mathbf{v} \in \mathscr{C}$ and $\alpha\mathbf{u} \in \mathscr{C}$ (see [21]). The *weight* of $\mathbf{u}$, wt($\mathbf{u}$), is the number of nonzero u_i. The *minimum weight* of $\mathscr{C}$ is

$d = \min\{\mathrm{wt}(\mathbf{u})\colon \mathbf{u} \neq 0, \mathbf{u} \in \mathscr{C}\}$. $\mathscr{C}$ is called an $[n, k]$ or $[n, k, d]$ code. The dot product is defined by $\mathbf{u} \cdot \mathbf{v} = \sum_{i=1}^{n} u_i v_i$ with the sum evaluated in $GF(4)$. The *dual* code $\mathscr{C}^{\perp} = \{\mathbf{v} = (v_1 \cdots v_n)\colon \mathbf{u} \cdot \mathbf{v} = 0 \text{ for all } \mathbf{u} \in \mathscr{C}\}$ is an $[n, n-k]$ code. All codes in this paper are linear codes over $GF(4)$ unless stated otherwise. An overbar denotes *conjugation*; that is, if $x \in GF(4)$ then $\bar{x} = x^2$. A similar notation is used for vectors, codes, etc. Thus $\bar{\mathbf{u}} = (\bar{u}_1 \cdots \bar{u}_n)$, $\bar{\mathscr{C}} = \{\bar{\mathbf{u}}\colon \mathbf{u} \in \mathscr{C}\}$.

The *direct sum* of $\mathscr{C}$ and $\mathscr{D}$ is $\mathscr{C} \oplus \mathscr{D} = \{|\, \mathbf{u} \,|\, \mathbf{v} \,|\colon \mathbf{u} \in \mathscr{C}, \mathbf{v} \in \mathscr{D}\}$, where $|\, \mathbf{u} \,|\, \mathbf{v} \,|$ denotes concatenation of $\mathbf{u}$ and $\mathbf{v}$. If $\mathscr{C} = \mathscr{D} \oplus \mathscr{E}$ with $\mathscr{D} \neq \varnothing$, $\mathscr{E} \neq \varnothing$ then $\mathscr{C}$ is called *decomposable*, otherwise *indecomposable*.

Let A_i be the number of code words of weight i in $\mathscr{C}$. Then $W_{\mathscr{C}}(x, y) = \sum_{i=0}^{n} A_i x^{n-i} y^i$ is the *weight enumerator* of $\mathscr{C}$. The *complete weight enumerator* (c.w.e.) of $\mathscr{C}$ is the polynomial

$$\mathrm{cwe}_{\mathscr{C}}(w, x, y, z) = \sum_{i,j,k,l} A_{ijkl} w^i x^j y^k z^l,$$

where A_{ijkl} is the number of code words in $\mathscr{C}$ containing i 0's, j 1's, k α's, and l β's. Clearly $W_{\mathscr{C}}(x, y) = \mathrm{cwe}_{\mathscr{C}}(x, y, y, y)$.

A *monomial* matrix M is a square matrix over $GF(4)$ with exactly one nonzero entry in each row and column. If M is $n \times n$, and $\mathscr{C}$ has length n, then M sends $\mathscr{C}$ to $\mathscr{C}M = \{\mathbf{u}M\colon \mathbf{u} \in \mathscr{C}\}$. Clearly there are $3^n n!$ monomials M. Some M's send $\mathscr{C}$ to itself: these form the *monomial* or *automorphism group* of $\mathscr{C}$ denoted by

$$\mathrm{Aut}(\mathscr{C}) = \{M\colon \mathscr{C}M = \mathscr{C}\}.$$

The other M's send $\mathscr{C}$ to a code $\mathscr{D} = \mathscr{C}M \neq \mathscr{C}$. $\mathscr{D}$ is said to be *monomially equivalent* (or simply *equivalent*) to $\mathscr{C}$, and we write $\mathscr{D} \approx \mathscr{C}$. The number of distinct codes which are monomially equivalent to $\mathscr{C}$ (including $\mathscr{C}$ itself) is

$$3^n n! / |\, \mathrm{Aut}(\mathscr{C})|. \tag{1}$$

Note that $\mathrm{Aut}(\mathscr{C})$ always contains the scalar matrices I, αI, βI. Equivalent codes have the same weight enumerator, but need not have the same complete weight enumerator.

$\mathscr{C}$ is called *even* if all code words have even weight. $\mathscr{C}$ is *formally self-dual* (f.s.d.) if $\mathscr{C}$ and $\mathscr{C}^{\perp}$ have the same weight enumerator $W_{\mathscr{C}}(x, y)$ (they need not have the same c.w.e.). $\mathscr{C}$ is *weakly self-dual* if $\mathscr{C} \subset \mathscr{C}^{\perp}$, and (*strictly*) *self-dual* if $\mathscr{C} = \mathscr{C}^{\perp}$. Clearly a strictly self-dual code is f.s.d. For an f.s.d. code $k = \frac{1}{2}n$, so n must be even. The aim of this paper is to study even f.s.d. codes: these comprise the third case of the aforementioned theorem of Gleason *et al.* Note that if $\mathscr{C}$ is an even f.s.d. code and M is a monomial matrix, then $\mathscr{C}M$ is an even f.s.d. code equivalent to $\mathscr{C}$.

Symbols. The subscript of a code (d_n, e_5, etc.) gives its length. Capital Roman letters (E_n, B_{10}, etc.) usually denote even f.s.d. codes. **1** is the vector $(1\ 1\ \cdots\ 1)$, I is usually an identity matrix, and B^T denotes the transpose of the matrix B.

2. Basic Properties of Even f.s.d. Codes

We begin with some elementary results.

THEOREM 1. *Let $\mathscr{C}$ be a linear code over GF(4). The following statements are equivalent.*

(i) *$\mathscr{C}$ is even.*

(ii) $\mathbf{u} \cdot \bar{\mathbf{u}} = 0$ *for all* $\mathbf{u} \in \mathscr{C}$.

(iii) $\mathbf{u} \cdot \bar{\mathbf{v}} = 0$ *for all* $\mathbf{u}, \mathbf{v} \in \mathscr{C}$.

(iv) $\bar{\mathscr{C}} \subseteq \mathscr{C}^{\perp}$.

Proof. Suppose $\mathbf{u} \in \mathscr{C}$ contains i 0's, j 1's, k α's, and l β's. Then wt($\mathbf{u}$) is even $\Leftrightarrow j + k + l$ is even $\Leftrightarrow \mathbf{u} \cdot \bar{\mathbf{u}} = 0$. Therefore (i) $\Leftrightarrow$ (ii). (iii) $\Leftrightarrow$ (iv) is immediate, as is (iii) $\Rightarrow$ (ii). To show (ii) $\Rightarrow$ (iii), suppose $\mathbf{u}, \mathbf{v} \in \mathscr{C}$. Then $(\mathbf{u} + \mathbf{v}) \cdot \overline{(\mathbf{u} + \mathbf{v})} = 0 \Rightarrow \mathbf{u} \cdot \bar{\mathbf{v}} = \bar{\mathbf{u}} \cdot \mathbf{v}$ and $(\alpha\mathbf{u} + \mathbf{v}) \cdot \overline{(\alpha\mathbf{u} + \mathbf{v})} = 0 \Rightarrow \mathbf{u} \cdot \bar{\mathbf{v}} = \alpha\bar{\mathbf{u}} \cdot \mathbf{v} \Rightarrow \bar{\mathbf{u}} \cdot \mathbf{v} = 0$. Q.E.D.

COROLLARY 2. *If $\mathscr{C}$ is an even $[n, k]$ code then $k \leqslant \frac{1}{2}n$.*

COROLLARY 3. *If $\mathscr{C}$ is an even $[n, \frac{1}{2}n]$ code then all coordinate places are used (i.e., no coordinate is zero in every code word).*

THEOREM 4. *If $\mathscr{C}$ is even and has dimension $k = \frac{1}{2}n$ (n even) then $\mathscr{C} = \bar{\mathscr{C}}^{\perp}$ and $\mathscr{C}$ is* f.s.d.

Proof. From Theorem 1(iv). Q.E.D.

THEOREM 5. *Suppose $\mathscr{C}$ is an even $[2m, m]$ code. By permuting the coordinates of $\mathscr{C}$ if necessary we can find a generator matrix for $\mathscr{C}$ in the form $[I \mid B]$, where I and B are $m \times m$ matrices. (The rows span $\mathscr{C}$.) Then B satisfies*

$$B\bar{B}^T = I. \tag{2}$$

Proof. $\bar{\mathscr{C}}$ has generator matrix $[I \mid \bar{B}]$, and $\bar{\mathscr{C}} = \mathscr{C}^{\perp}$ implies (2). Q.E.D.

THEOREM 6. *An even code which is strictly self-dual has a generator matrix consisting of* 0*'s and* 1*'s.*

Proof. $\mathscr{C} = \mathscr{C}^{\perp} = \bar{\mathscr{C}}$ implies $B = \bar{B}$. Q.E.D.

If $\mathscr{C}$ is a code over $GF(4)$ let $\mathscr{C}_0 = \{\mathbf{u} \in \mathscr{C}; \mathbf{u} = \bar{\mathbf{u}}\}$ be the binary subcode. Thus $\mathscr{C}_0$ is a linear code over $GF(2)$.

THEOREM 7. *$\mathscr{C} = \bar{\mathscr{C}}$ if and only if $\mathscr{C}$ is the $GF(4)$ span of $\mathscr{C}_0$.*

Proof (Only if). Any $\mathbf{u} \in \mathscr{C}$ can be written as $\mathbf{u} = \mathbf{s} + \beta\mathbf{t}$, where $\mathbf{s} = \alpha\mathbf{u} + \beta\bar{\mathbf{u}}$ and $\mathbf{t} = \mathbf{u} + \bar{\mathbf{u}}$ are in $\mathscr{C}_0$. Q.E.D.

We now consider the weight enumerators of these codes.

THEOREM 8 [17, 21]. *If $\mathscr{C}$ is an $[n, k]$ linear code over $GF(4)$ then*

$$W_{\mathscr{C}^{\perp}}(x, y) = \frac{1}{4^k} W_{\mathscr{C}}(x + 3y, x - y), \tag{3}$$

$$\mathrm{cwe}_{\mathscr{C}^{\perp}}(w, x, y, z) = \frac{1}{4^k} \mathrm{cwe}_{\mathscr{C}}(w + x + y + z, w - x + y - z, w + x - y - z, w - x - y + z). \tag{4}$$

COROLLARY 9. *If $\mathscr{C}$ is an even code of length n then $\mathscr{C}^{\perp}$ contains a vector of weight n. Hence if $\mathscr{C}$ is even* f.s.d. *there is a code $\mathscr{D} \approx \mathscr{C}$ with $\mathbf{1} \in \mathscr{D}$ such that $\sum u_i = 0$ for all $\mathbf{u} \in \mathscr{D}$. (This gives another proof of Corollary* 3.)

Proof. From (3) the number of vectors of weight n in $\mathscr{C}^{\perp}$ is $4^{-k} \sum A_i 3^{n-i} > 0$. Q.E.D.

COROLLARY 10. *Let $\mathscr{C}$ be an $[n, k]$ code over $GF(4)$, let N_i be the number of code words in $\mathscr{C}^{\perp}$ containing exactly i 1's, and let $A_j^{(0)}$ (resp. $A_j^{(n)}$) be the number of code words $\mathbf{u} \in \mathscr{C}$ of weight j with $\sum u_i = 0$ (resp. $\neq 0$). Then*

$$\sum_{i=0}^{n} N_i x^i = \frac{1}{4^k} \sum_{j=0}^{n} \left(A_j^{(0)} - \frac{1}{3} A_j^{(n)}\right) (x + 3)^{n-j} (x - 1)^j.$$

Proof. From (4). Q.E.D.

COROLLARY 11. *Let $\mathscr{C}$ be an even f.s.d. code which contains $\mathbf{1}$ and has weight enumerator $\sum A_j x^{n-j} y^j$. Then the number of code words in $\mathscr{C}$ with exactly i 1's is A_{n-i}.*

COROLLARY 12. *If $\mathscr{C}$ is f.s.d. then $W_{\mathscr{C}}(x, y)$ is fixed under the linear substitution*

$$\text{replace } \begin{pmatrix} x \\ y \end{pmatrix} \quad \text{by} \quad \frac{1}{2} \begin{pmatrix} 1 & 3 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}, \tag{5}$$

and $\mathrm{cwe}_{\mathscr{C}}(w, x, y, z)$ *is fixed under the linear substitution*

$$\textit{replace} \begin{pmatrix} w \\ x \\ y \\ z \end{pmatrix} \quad \textit{by} \quad \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}\begin{pmatrix} w \\ x \\ y \\ z \end{pmatrix}. \tag{6}$$

The next theorem characterizes the weight enumerators of even f.s.d. codes.

THEOREM 13 [20]. *Let* $\mathscr{C}$ *be an even f.s.d. code. Then the weight enumerator of* $\mathscr{C}$ *is a polynomial in*

$$\eta_2 = x^2 + 3y^2 \qquad \textit{and} \qquad \theta_6 = y^2(x^2 - y^2)^2. \tag{7}$$

Sketch of proof. (The method is described in [20, 32, 33]; see also [16].) By hypothesis (using (5)), $W_{\mathscr{C}}(x, y)$ is invariant under the group $\mathscr{G}$ generated by $\frac{1}{2}\left(\begin{smallmatrix} 1 & 3 \\ 1 & -1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. $\mathscr{G}$ is isomorphic to the dihedral group of order 12, and has Molien series $1/\{(1 - \lambda^2)(1 - \lambda^6)\}$. The ring of invariants of $\mathscr{G}$ is a free ring with two generators, for which we may take the weight enumerators of the codes C_2 and E_6 below, η_2 and $\eta_6 = x^6 + 45x^2y^4 + 18y^6$, or the equivalent pair η_2 and $\theta_6 = \frac{1}{9}(\eta_2^3 - \eta_6)$. Q.E.D.

Hence if $\mathscr{C}$ is an even f.s.d. $[n, \frac{1}{2}n]$ code, where $n = 6m + 2v$, $v = 0$, 1, or 2, then

$$W_{\mathscr{C}}(x, y) = \sum_{i=0}^{m} a_i \eta_2^{(1/2)n-3i} \theta_6{}^i \tag{8}$$

for suitable rational numbers a_i. Suppose the numbers $a_0, \ldots, a_m$ are chosen so that the right-hand side of (8) becomes

$$x^n + 0 \cdot x^{n-1}y + \cdots + 0 \cdot x^{n-2m-1}y^{2m+1} + A^*_{2m+2}x^{n-2m-2}y^{2m+2} + A^*_{2m+4}x^{n-2m-4}y^{2m+4} + \cdots = \eta_n \qquad \text{(say)}. \tag{9}$$

This determines the a_i uniquely. η_n is called an *extremal weight enumerator* [24, 26]. If $A^*_{2m+2} \neq 0$, then $\mathscr{C}$ has minimum weight $\leqslant 2m + 2$, and if $\mathscr{C}$ has minimum weight $= 2m + 2$, then $W_{\mathscr{C}}(x, y) = \eta_n$. Table I shows η_n for $n \leqslant 24$ and $n = 30$.

TABLE I

Coefficients of the Extremal Weight Enumerators η_n

	Length n							
	2	4	6	8	10	12	14	16
	Code							
Weight	C_2	$2C_2$	E_6	E_8	E_{10}, B_{10}	None	Q_{14}	R_{16}
0	1	1	1	1	1	1	1	1
2	3	6	0	0	0	0	0	0
4		9	45	42	30	0	0	0
6			18	168	300	396	273	168
8				45	585	1485	2457	2610
10					108	1980	7098	14448
12						234	6006	29400
14							549	17640
16								1269

	Length n				
	18	20	22	24	30
	Code				
Weight	S_{18}	?	?	?	Q_{30}
0	1	1	1	1	1
8	2754	1710	990	0	0
10	18360	20976	18480	18216	0
12	77112	126540	163548	156492	118755
14	110160	355680	728640	1147608	1151010
16	50949	395865	1533609	3736557	12038625
18	2808	141360	1349040	6248088	61752600
20		6444	385308	4399164	195945750
22			14688	1038312	341403660
24				32778	312800670
26					129570840
28					18581895
30					378018

THEOREM 14. *Let* $n = 6m + 2\nu$, $\nu = 0, 1,$ *or* 2. *The coefficient of* $x^{n-2m-2}y^{2m+2}$ *in the extremal weight enumerator* η_n *is given by*:

$$A^*_{2m+2} = \frac{18(6m-1)}{m+1}\binom{3m}{m-1} \quad \text{if } \nu = 0,$$

$$= \frac{3(6m+1)}{m+1}\binom{3m+1}{m} \quad \text{if } \nu = 1,$$

$$= 3\binom{3m+2}{m+1} \quad \text{if } \nu = 2.$$

Proof. Parallel to that of [26, Theorem 2]. Theorem 14 may be considered as a missing "Case 4" of that paper, corresponding to the parameters $\alpha = 3$, $w = 2$, $R = 3$, $S = 2$, $f = 1 + \alpha y$, $g = y(1-y)^w$. Q.E.D.

Since $A^*_{2m+2} > 0$ we have:

COROLLARY 15. *The minimum weight of an even f.s.d. code* $\mathscr{C}$ *satisfies*

$$d \leqslant 2[n/6] + 2. \tag{10}$$

If $d = 2[n/6] + 2$, $W_{\mathscr{C}}(x, y) = \eta_n$.

This bound is attained for $n = 2$, 4, 6, 8, 10, 14, 16, 18, and 30, but not 12 (see Section 4). Table II compares the highest minimum weights $d_{\max}$ of even f.s.d. and even self-dual codes for $n \leqslant 32$. In view of Theorem 6 the information about even self-dual codes follows from the corresponding results for binary self-dual codes given in [10, 26, 28, 30, 35].

For larger values of n we have:

THEOREM 16. (a) A_{2m+4} (*the third nonzero coefficient in* η_n) *is negative for* $n \geqslant 102$ *if* $\nu = 0$, *for* $n \geqslant 122$ *if* $\nu = 1$ *and for* $n \geqslant 136$ *if* $\nu = 2$. *Therefore no code has weight enumerator* η_n *for these values of n.*

(b) *Let b be any constant. Suppose the* a_i *in* (8) *are chosen so that the right-hand side of* (8) *becomes*

$$x^n + A_d x^{n-d}y^d + A_{d+2}x^{n-d-2}y^{d+2} + \cdots,$$

where $d \geqslant 2[n/6] + 2 - 2b$. *Then one of the coefficients* $A_d, A_{d+2}, \ldots$ *is negative, for all sufficiently large n.*

Proof. Parallel to that of [24, Theorem 2]. Q.E.D.

We can also obtain a partial characterization of the complete weight enumerators.

TABLE II

The Highest Minimum Weight $d_{\max}$ of Even f.s.d. and Even Self-Dual Codes Over $GF(4)$

Length n	Dim k	Even f.s.d. $d_{\max}$	Even f.s.d. Code	Even self-dual $d_{\max}$	Even self-dual Code
2	1	2	C_2	2	C_2
4	2	2	$2C_2$	2	$2C_2$
6	3	4	E_6	2	$3C_2$
8	4	4	E_8	4	E_8
10	5	4	E_{10}, B_{10}	2	$C_2 \oplus E_8$
12	6	4	Table V	4	E_{12}
14	7	6	Q_{14}	4	G_{14}
16	8	6	R_{16}	4	[28]
18	9	8	S_{18}	4	[28]
20	10	$\leqslant 8$	?	4	[28]
22	11	$\leqslant 8$	?	6	[30]
24	12	$\leqslant 10$	?	8	Golay
26	13	$\leqslant 10$	?	6	[26]
28	14	$\leqslant 10$	?	6	[35]
30	15	12	Q_{30}	6	[35]
32	16	$\leqslant 12$	?	8	[35]

THEOREM 17. *Let $\mathscr{C}$ be an even f.s.d. code which contains the code word* **1** *(see Corollary* 8*). Then the c.w.e. of $\mathscr{C}$ is a polynomial in f_2, f_6, f_8, and f_{12}, where (using standard notation for symmetric functions of w, x, y, z)*

$$f_2 = (2) = w^2 + x^2 + y^2 + z^2, \tag{11}$$

$$f_6 = (6) + 15(222) = w^6 + \cdots + 15(w^2x^2y^2 + \cdots), \tag{12}$$

$$f_8 = (8) + 14(44) + 168(2222), \tag{13}$$

$$f_{12} = (12) + 22(66) + 330(6222) + 165(444) + 330(4422). \tag{14}$$

Proof. The c.w.e. is invariant under the group $\mathscr{G}$ generated by

$$H = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & & & \\ & -1 & & \\ & & -1 & \\ & & & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

$\mathscr{G}$ consists of the 1152 matrices $\pm DP$ and $\pm DH\Pi D'$, where D, $D' = \mathrm{diag}\{1, \pm 1, \pm 1, \pm 1\}$, P is any 4×4 permutation matrix, and Π is any 4×4 permutation matrix with a 1 in the top left corner. It follows that $\mathscr{G}$ is the classical group [3, 4, 3], the group of the 24-cell [11]. The Molien series is $1/\{(1 - \lambda^2)(1 - \lambda^6)(1 - \lambda^8)(1 - \lambda^{12})\}$, and the ring of invariants is a free ring with four generators. To find a set of generators we compute the c.w.e.'s

of the codes C_2, E_6, E_8, and C_{12} below, which are, respectively, f_2, f_6, f_8, and

$$\frac{-161}{144}f_2^6 + \frac{49}{36}f_2^3f_6 + \frac{11}{45}f_6^2 + \frac{21}{16}f_2^2f_8 - \frac{4}{5}f_{12}. \tag{15}$$

Q.E.D.

The *support* of a vector $\mathbf{u}$ is the set of coordinate places i where $u_i \neq 0$. Of course $\mathbf{u}$, $\alpha\mathbf{u}$, and $\beta\mathbf{u}$ have the same support. In some cases the supports of code words form t-designs.

THEOREM 18. (a) *Let $\mathscr{C}$ be an even f.s.d.* $[6m, 3m, 2m + 2]$ *code. Then the supports (with duplicates omitted) of the code words of weights*

$$2m + 2, 2m + 4, \ldots, 2[(3m + 2)/2] \tag{16}$$

form 5-designs. In particular, the code words of weight $2m + 2$ support a $t - (v, k, \lambda)$ design with parameters

$$5 - \left(6m, 2m + 2, \binom{3m - 3}{m - 2}\right). \tag{17}$$

(b) *Let $\mathscr{C}$ be an even f.s.d.* $[6m + 2, 3m, 2m + 2]$ *code. Then the code words of weights given by* (16) *support 3-designs.*

Proof. This is a special case of the main theorem of Assmus and Mattson [1] (see also [21, Ch. 6, Theorem 29 and Corollary 30]). The parameters (17) follow from Theorem 14 above. Q.E.D.

EXAMPLES. The code words of weights 8 and 10 in S_{18} below support 5-designs with parameters

$$5 - (18, 8, 6) \quad \text{and} \quad 5 - (18, 10, 180). \tag{18}$$

The code words of weights 12, 14, and 16 in Q_{30} support

$$5 - (30, 12, 220), \quad 5 - (30, 14, 5390), \quad \text{and} \quad 5 - (30, 16, 123000) \tag{19}$$

designs. (The designs (19)—although not the values of λ—were given by Assmus and Mattson in [3].) For $n = 24$ see Open Problem (2) below.

OPEN PROBLEMS. (1) If $\mathscr{C}$ is an even f.s.d. code with a *binary* generator matrix, are there additional constraints that its weight enumerator must satisfy? Is the weight enumerator related to that of the binary code with the same generator matrix? (Tables I, IV, and V and [28, 30] provide relevant data.)

(2) Remove the question marks in Tables I and II. In particular, is there a [24, 12, 10] even f.s.d. code with weight enumerator η_{24} ? In view of Theorem 18, the code words of weights 10, 12, and 14 would give rise to new 5-designs. No linear code has weight enumerator η_{12} (Table V), but what about a nonlinear code? (This question is prompted by the existence of the Nordstrom–Robinson code in the binary case [26, p. 195].)

(3) In Theorem 18, do the code words of weights greater than (16) also support t-designs?

3. Enumeration of Even f.s.d. Codes

There are three distinct even f.s.d. codes of length 2, spanned, respectively, by the vectors (11), (1α) and (1β). These are monomially equivalent however. In general, let $N_d(n)$ be the number of *distinct* even f.s.d. codes of length n, $N_m(n)$ the number of *monomially inequivalent* even f.s.d. codes, and $N_i(n)$ the number of monomially inequivalent *indecomposable* even f.s.d. codes. Thus $N_d(2) = 3$, $N_m(2) = N_i(2) = 1$. These numbers are given in Table III for $n \leqslant 14$. The values of $N_d(n)$ follow from Theorem 19, and those of $N_m(n)$, $N_i(n)$ from Section 4.

TABLE III

The Number of Even f.s.d. Codes[a]

n	$N_d(n)$	$N_m(n)$	$N_i(n)$
2	3	1	1
4	27	1	0
6	891	2	1
8	114939	3	1
10	58963707	5	2
12	120816635643	10	4
14	989850695823099	21	10

[a] $N_d(n)$ = number of *distinct* even f.s.d. codes of length n, $N_m(n)$ = number of *monomially inequivalent* even f.s.d. codes, and $N_i(n)$ = number of monomially inequivalent *indecomposable* even f.s.d. codes.

Theorem 19.

$$N_d(n) = \prod_{i=0}^{(1/2)n-1} (2^{2i+1} + 1). \tag{20}$$

This result is classical: It is the number of totally isotropic subspaces with respect to a unitary polarity in the projective geometry of dimension

$n-1$ over $GF(4)$ (see Dembowski [11a, p. 47] for numerous references). Another proof follows from the next two lemmas. In both, $\mathscr{C}$ is an even $[n, k]$ code.

LEMMA 20. *The number of even weight vectors in $\mathscr{C}^\perp$ is*

$$\tfrac{1}{2}(4^{n-k} + (-2)^n). \tag{21}$$

Proof. Follows from (3). In particular, the number of even weight vectors in $GF(4)^n$ is $\frac{1}{2}(4^n + (-2)^n)$.

LEMMA 21. *A coset $\mathscr{C} + \mathbf{a}$ of $\mathscr{C}$ in $\bar{\mathscr{C}}^\perp$ contains only even weight vectors if $\mathbf{a}$ has even weight, and only odd weight vectors if $\mathbf{a}$ has odd weight.*

Proof. For $\mathbf{c} \in \mathscr{C}$ and $\mathbf{a} \in \bar{\mathscr{C}}^\perp$,

$$\mathrm{wt}(\mathbf{a} + \mathbf{c}) \equiv (\mathbf{a} + \mathbf{c}) \cdot (\bar{\mathbf{a}} + \bar{\mathbf{c}}) = \mathbf{a} \cdot \bar{\mathbf{a}} \pmod 2 \qquad \text{Q.E.D.}$$

Proof of Theorem 19. Let $\mathscr{C}$ be an even $[n, k]$ code with n even and $k < \frac{1}{2}n$. Let $\mathbf{u}$ be an even weight vector in $\bar{\mathscr{C}}^\perp - \mathscr{C}$. Then $\mathscr{C} \cup \{\mathbf{u} + \mathscr{C}\} \cup \{\alpha\mathbf{u} + \mathscr{C}\} \cup \{\beta\mathbf{u} + \mathscr{C}\}$ is an $[n, k+1]$ even code containing $\mathscr{C}$, which in fact contains $\frac{1}{3}(4^{k+1} - 1)$ distinct $[n, k]$ codes. Let $N_d(n, k)$ be the number of distinct even $[n, k]$ codes, so that $N_d(n) = N_d(n, \frac{1}{2}n)$. Then

$$N_d(n, k+1) = \frac{4^{n-2k} + 2^{n-2k} - 2}{2(4^{k+1} - 1)} N_d(n, k). \tag{22}$$

Equation (20) then follows using $N_d(n, 1) = \frac{1}{6}(4^n + 2^n - 2)$. Q.E.D.

Theorem 19 and Eq. (1) together imply:

THEOREM 22.

$$N_d(n)/3^{n-1}n! \leqslant N_m(n) \leqslant N_d(n), \tag{23}$$

$$\log_2 N_m(n) = (n^2/4)(1 + o(1)). \tag{24}$$

In particular, $N_m(24) > 10^9$, so it will be difficult to settle the existence of a [24, 12, 10] code by extending the enumeration in Section 4 to $n = 24$.

THEOREM 23. *Let $\mathbf{a}$ be a nonzero even weight vector of length n. The number of even f.s.d. codes containg $\mathbf{a}$ is*

$$M(n) = \prod_{i=0}^{(1/2)n-2} (2^{2i+1} + 1). \tag{25}$$

The proof is similar to that of Theorem 19 and is omitted.

THEOREM 24. *Let* $S_n(x, y) = \sum W_{\mathscr{C}}(x, y)$, *where the sum extends over all even f.s.d. codes of length n. Then*

$$S_n(x, y) = M(n) \cdot [2^{n-1}x^n + \tfrac{1}{2}\{(x + 3y)^n + (x - 3y)^n\}]. \tag{26}$$

Proof. Evaluate the following sum in two ways, using Theorems 19 and 23:

$$\sum_{\mathscr{C}} \sum_{\mathbf{u} \in \mathscr{C}} x^{n-\mathrm{wt}(\mathbf{u})} y^{\mathrm{wt}(\mathbf{u})}. \qquad \text{Q.E.D.}$$

Theorems 19 and 23 also imply via a standard argument that even f.s.d. codes exist which asymptotically meet the Gilbert–Varshamov bound (compare [21, Chap. 17, Theorem 31]).

In the course of proving Theorem 19 we also found the number of even $[n, k]$ codes (which therefore satisfy $\mathscr{C} \subset \mathscr{C}^{\perp}$). We conclude this section with:

THEOREM 25. *The number of even* $[n, k]$ *codes* $\mathscr{C}$ *which satisfy* $\mathscr{C} \subset \mathscr{C}^{\perp}$ *is given by*

$$L(n, k) = \sum_{m=0}^{k} \frac{2^{m^2}(2^{n-k-m} - 1) \prod_{i=1}^{k+m-1} (2^{n-2i} - 1)}{\prod_{i=1}^{m} (2^{2i} - 1) \prod_{i=1}^{k-m} (2^i - 1)}. \tag{27}$$

The proof depends on the following lemma.

LEMMA 26. *Let* V *be a vector space of dimension* $2m$ *over* $GF(4)$. *Suppose* $V = \overline{V}$. *Then the number of subspaces* W *of* V *of dimension* m *for which* $W + \overline{W} = V$ (*so that* $W \cap \overline{W} = 0$) *is*

$$K(m) = 2^{m^2} \prod_{i=0}^{m-1} (2^{2i+1} - 1). \tag{28}$$

Proof. As in Theorem 7, V is spanned by $V_0 = \{\mathbf{b} \in V: \mathbf{b} = \bar{\mathbf{b}}\}$. We first determine the number $g(m)$ of m-tuples $\mathbf{a}_1, \ldots, \mathbf{a}_m$ of members of V such that $\mathbf{a}_1, \ldots, \mathbf{a}_m, \bar{\mathbf{a}}_1, \ldots, \bar{\mathbf{a}}_m$ span V. If $\mathbf{a} \in V$, $\mathbf{a} \neq 0$, then $\mathbf{a}$ and $\bar{\mathbf{a}}$ are dependent if and only if $\mathbf{a} = \xi\mathbf{b}$ with $\xi \in GF(4)$, $\mathbf{b} \in V_0$. Thus the number of $\mathbf{a}$ with $\mathbf{a}$ and $\bar{\mathbf{a}}$ independent is $(4^{2m} - 1) - 3(2^{2m} - 1) = (2^{2m} - 1)(2^{2m} - 2)$, so that $g(1) = (2^2 - 1)(2^2 - 2)$. Having chosen $\mathbf{a}_1$, we form $V/\langle \mathbf{a}_1, \bar{\mathbf{a}}_1 \rangle$. By induction, the number of $(m - 1)$-tuples of the desired sort in $V/\langle \mathbf{a}_1, \bar{\mathbf{a}}_1 \rangle$ is $g(m - 1)$. Since each member of $V/\langle \mathbf{a}_1, \bar{\mathbf{a}}_1 \rangle$ has 4^2 preimages in V, we get

$$g(m) = (2^{2m} - 1)(2^{2m} - 2)\, 4^{2(m-1)} g(m - 1),$$

which yields

$$g(m) = 4^{m(m-1)} \prod_{i=1}^{m} (2^{2i} - 1)(2^{2i} - 2). \tag{29}$$

Each m-tuple of the sort described spans a subspace W of the required kind, so that $K(m)$ is $g(m)$ divided by the number of bases of such a W,

$$K(m) = g(m) \Big/ \prod_{i=0}^{m-1} (4^m - 4^i),$$

and that gives (28). Q.E.D.

Proof of Theorem 25. Let $\mathscr{A} = \mathscr{C} + \bar{\mathscr{C}}$ have dimension $k + m$. By Theorem 7, $\mathscr{A}$ is spanned by its binary subcode $\mathscr{A}_0$. Similarly $\mathscr{B} = \mathscr{C} \cap \bar{\mathscr{C}}$ has dimension $k - m$ and is spanned by $\mathscr{B}_0$, and we have the following picture:

$$\begin{array}{ccccc} \mathscr{C} + \bar{\mathscr{C}} & & = \mathscr{A} & & \dim k + m, \\ & \diagup \quad \diagdown & & & \\ \mathscr{C} & & \bar{\mathscr{C}} & & \dim k, \\ & \diagdown \quad \diagup & & & \\ \mathscr{C} \cap \bar{\mathscr{C}} & & = \mathscr{B} & & \dim k - m. \end{array}$$

Thus $\mathscr{C}$ is associated with two binary codes $\mathscr{A}_0$ and $\mathscr{B}_0$ with $\mathscr{B}_0 \subseteq \mathscr{A}_0 \subseteq \mathscr{A}_0^{\perp}$. Conversely, given binary codes $\mathscr{A}_0$, $\mathscr{B}_0$ with $\mathscr{B}_0 \subseteq \mathscr{A}_0 \subseteq \mathscr{A}_0^{\perp}$, we create such a $\mathscr{C}$ by taking $\mathscr{A}$ and $\mathscr{B}$ to be the codes over $GF(4)$ spanned by $\mathscr{A}_0$ and $\mathscr{B}_0$, and choosing $\mathscr{B} \subseteq \mathscr{C} \subseteq \mathscr{A}$ with $\mathscr{C}/\mathscr{B}$ a subspace of $\mathscr{A}/\mathscr{B}$ as in the lemma. Let $L(n, k, m)$ be the number of such $\mathscr{C}$ with $\dim(\mathscr{C} + \bar{\mathscr{C}}) = k + m$. Then $L(n, k) = \sum L(n, k, m)$, and

$$L(n, k, m) = (\text{number of } [n, k + m] \text{ binary codes } \mathscr{A}_0 \subseteq \mathscr{A}_0^{\perp}) \times (\text{number of } [n, k - m] \text{ subcodes } \mathscr{B}_0 \subseteq \mathscr{A}_0) \times K(m).$$

The first factor is given in [30, Corollary 3.8], and the second is well known. Q.E.D.

OPEN PROBLEMS (continued). (4) What is the average order of $\mathrm{Aut}(\mathscr{C})$ for even f.s.d. codes $\mathscr{C}$ of length n? Is $|\mathrm{Aut}(\mathscr{C})| = 3$ possible?

4. EVEN f.s.d. CODES OF LENGTH UP TO 14

The main goal of this section is to prove:

THEOREM 27. *All indecomposable even f.s.d. codes over GF(4) of length* $\leqslant 14$ *are shown in Table* V. *The corresponding values of* $N_m(n)$ *and* $N_i(n)$ *are shown in Table* II.

TABLE IV

Some Special Indecomposable Codes

$d_m (m = 4, 6, 8, \ldots)$:

0	1	2	3	4	5	$\cdots$
1	1	1	1			0
		1	1	1	1	
		.	.	.	.	.
	0			1	1	1	1

parameters $[m, \frac{1}{2}m - 1, 4]$, $W = \frac{1}{4}[(x^2 + 3y^2)^{m/2} + 3(x^2 - y^2)^{m/2}]$,

$$A_{2r} = \tfrac{1}{4}(3^r + 3(-1)^r)\binom{m/2}{r}, \quad g = 3 \cdot 2^{m/2}(m/2)! \qquad (m \geq 6),$$

with generators (01), (02)(13), (024...)(135...).

e_5:

0	1	2	3	4
1	1	1	1	0
0	1	α	β	1

, parameters [5, 2, 4], $W = x^4 + 15y^4$,

$g = 3 \mid \mathscr{A}_5 \mid = 180$, with generators (01)(23), (01234) diag$\{1\alpha\beta 1\alpha\}$.

E_6:

1	1	1	1	0	0
0	0	1	1	1	1
1	0	1	0	α	β

or equivalently

0	1	2	3	4	5
1	0	0	1	α	α
0	1	0	α	1	α
0	0	1	α	α	1

,

parameters [6, 3, 4], $W = \eta_6$, $cwe = f_6$, $g = 3 \mid \mathscr{A}_6 \mid = 1080$, with generators (02134), (235) diag$\{1\beta\alpha\beta\alpha 1\}$ ($\mathscr{A}_6$ is the alternating group on six letters).

e_7:

0	1	2	3	4	5	6
1	1	1	1	0	0	0
0	0	1	1	1	1	0
1	0	1	0	1	0	1

, parameters [7, 3, 4], $W = x^6 + 21x^2y^4 + 42y^6$,

$g = 3 \cdot 7 \cdot 6 \cdot 4 = 504$, with generators (01)(23), (0146253).

E_8:

0	1	2	3	4	5	6	7
1	1	1	1	0	0	0	0
0	0	1	1	1	1	0	0
0	0	0	0	1	1	1	1
1	0	1	0	1	0	1	0

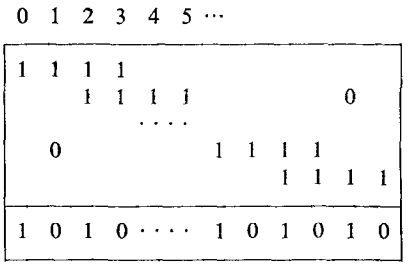
, parameters [8, 4, 4], $W = \eta_8$, $cwe = f_8$,

$g = 3 \cdot 8 \cdot 7 \cdot 6 \cdot 4 = 4032$, with generators (01)(67), (0146253).

Table continued

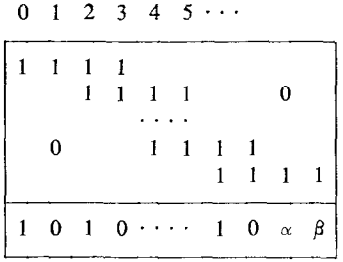
TABLE IV (*Continued*)

E_n :



$(n = 12, 16, 20,...)$

or



$(n = 10, 14, 18,...)$,

parameters $[n, \frac{1}{2}n, 4]$, $A_4 = 3\binom{n/2}{2}$, $g = 3 \cdot 2^{n/2-1}(n/2)!$, with generators (01)(23), (02)(13), (024...)(135...).

Theorems 28–30 are useful in classifying even f.s.d. codes. Their proofs are straightforward and are omitted.

THEOREM 28. *An even code with minimum distance* 2 *and length greater than* 2 *is decomposable.*

Table IV shows some codes which play a special role in the classification. For each code the table gives some or all of; the name of the code, a generator matrix, the parameters $[n, k, d]$, the weight enumerator W, the complete weight enumerator *cwe*, the number A_r of code words of weight r, the order g of the monomial group of the code, and generators for this group. The generators have the form $\pi\delta$, where π is a permutation and δ is a diagonal matrix. For example (13) diag$\{1\alpha\beta\}$ would mean first apply the permutation (13) to the coordinates, then multiply the coordinates by 1, α, and β respectively. The corresponding monomial matrix is

$$\begin{bmatrix} 0 & 0 & \beta \\ 0 & \alpha & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

TABLE V

Indecomposable Even f.s.d. Codes over $GF(4)$

Length 2

C_2 : [11], parameters [2, 1, 2], $W = \eta_2 = x^2 + 3y^2$, $cwe = f_2$, $g = 3 \cdot 2! = 6$.

Length 4 None.

Length 6 E_6 (Table IV).

Length 8 E_8 (Table IV).

Length 10

(i) E_{10} (Table IV), $W = \eta_{10}$, $g = 3 \cdot 2^4 \cdot 5! = 5760$

(ii) B_{10}

$\begin{matrix}1&1&1&1&0\\0&1&\alpha&\beta&1\end{matrix}$		0
0		$\begin{matrix}1&1&1&1&0\\0&1&\alpha&\beta&1\end{matrix}$
$\begin{matrix}0&1&\beta&\alpha&0\end{matrix}$		$\begin{matrix}0&1&\beta&\alpha&0\end{matrix}$

[10, 5, 4], $W = \eta_{10}$, $g = 3 \cdot 2 \cdot |\mathscr{A}_5|^2 = 21600$.

Length 12 (i) E_{12} (Table IV), $A_4 = 45$, $g = 3 \cdot 2^5 \cdot 6! = 69120$.

(ii) C_{12} :

$\begin{matrix}1&1&\alpha&\alpha&0\\0&1&1&\beta&\beta\end{matrix}$		0
0		$\begin{matrix}1&1&1&1&0&0&0\\0&0&1&1&1&1&0\\1&0&1&0&1&0&1\end{matrix}$
$\begin{matrix}0&\alpha&1&\alpha&0\end{matrix}$		$\begin{matrix}1&1&1&1&1&1&1\end{matrix}$

[12, 6, 4], $A_4 = 36$, cwe = Eq. (15),
$g = 3 \cdot |\mathscr{A}_5| \cdot 7 \cdot 6 \cdot 4 = 30240$.

(iii) D_{12} :

$\begin{matrix}1&1&1&1&0&0\\0&0&1&1&1&1\end{matrix}$		0
0		$\begin{matrix}1&1&1&1&0&0\\0&0&1&1&1&1\end{matrix}$
$\begin{matrix}1&0&1&0&1&0\\0&\alpha&\alpha&0&\alpha&0\end{matrix}$		$\begin{matrix}0&\alpha&\alpha&0&\alpha&0\\1&0&1&0&1&0\end{matrix}$

[12, 6, 4], ${}^{\tau}A_4 = 18$,
$g = 3 \cdot 2 \cdot (2^2 3!)^2 = 3456$.

Table continued

(iv) F_{12} :

0	1	2	3	4	5	6	7	8	9	10	11
1	1	1	1								
				1	1	1	1		0		
		0						1	1	1	1
1	1	0	0	1	1	0	0	1	1	0	0
1	0	1	0	1	0	1	0	α	α	0	0
1	0	1	0	β	β	0	0	1	0	1	0

[12, 6, 4], $A_4 = 9$,
$g = 3 \cdot 3! \cdot 4^3 \cdot 3^2 = 10368$, with generators
(04)(15)(26)(37)(89), (08)(19)(2, 10)(3, 11)(45),
(123)(567) diag$\{1^8\alpha^4\}$.

Length 14

(i) E_{14} (Table IV), $A_4 = 63$, $g = 3 \cdot 2^6 \cdot 7! = 967680$.

(ii) G_{14} :

e_7	0
0	e_7
1	1

, [14, 7, 4], $A_4 = 42$, $g = 3 \cdot 2 \cdot 168^2 = 169344$.

(iii) H_{14} :

1	1	1	1	0	0	0	0							0
0	0	1	1	1	1	0	0			0				0
0	0	0	0	1	1	1	1							0
								1	1	1	1	0		0
				0				0	1	α	β	1		0
0	0	0	0	0	0	1	1	0	1	β	α	0		1
1	0	1	0	1	0	α	β	0	0	0	0	0		1

[14, 7, 4], $A_4 = 33$, $g = 3(2^3 \cdot 4!) \mid \mathscr{A}_5 \mid = 34560$.

(iv) I_{14} :

0	1	2	3	4	5	6	7	8	9	10	11	12	13
1	1	1	1	0									
0	1	α	β	1			0					0	
			0		1	1	1	1	0				
					0	1	α	β	1				
0	0	0	0	0	0	0	0	0	0	1	1	1	1
0	1	β	α	0	0	0	0	0	0	1	α	β	0
0	0	0	0	0	0	1	β	α	0	1	β	α	0

[14, 7, 4], $A_4 = 33$, $g = 3 \cdot 2 \cdot \mid \mathscr{A}_5 \mid^2 \cdot \mid \mathscr{A}_4 \mid = 259200$
(since (10,11)(12, 13), (10, 12)(11, 13), and (10, 11, 12) diag$\{\beta^5\alpha^5 1^4\}$ generate an $\mathscr{A}_4$ on the last four coordinates).

Table continued

(v) J_{14} :

1 1 1 1 0 0 0 0 0 0 1 1 1 1 0 0 0 0 0 0 1 1 1 1		0
0		1 1 1 1 0 0 0 0 1 1 1 1
0 0 0 0 0 0 1 1 1 0 1 0 1 0 1 0		1 0 1 0 α β 0 0 0 0 1 1

[14, 7, 4], $A_4 = 27, g = 3(2^3 \cdot 4!)(2^2 \cdot 3!) = 13824$.

(vi) K_{14} :

1 1 1 1 0 0 0 0 1 1 1 1	0	0
0	1 1 1 1 0 0 0 0 1 1 1 1	0
0 0 0 0 1 1 1 0 1 0 α β 0 0 0 0 0 0	0 0 0 0 1 1 0 0 0 0 0 0 1 0 1 0 α β	α β 1 1 1 1

[14, 7, 4], $A_4 = 18, g = 3 \cdot 2 \cdot (2^2 \cdot 3!)^2 = 3456$.

(vii) L_{14} :

0 1 2 3	4 5 6 7	8 9 10 11 12 13
1 1 1 1 0	1 1 1 1	0 1 1 1 1 1 1 1 1
0 0 1 1 0 1 0 1 0 0 0 0	0 0 1 1 0 1 0 1 0 1 α β	0 0 1 1 0 0 0 0 0 0 β β 0 1 0 1 0 1

[14, 7, 4], $A_4 = 15, g = 3 \cdot 2 \cdot |\mathscr{A}_4| \cdot 4 \cdot (2^2 \cdot 3!) = 6912$, with generators (01)(23), (04)(15)(26)(37)(12, 13), (8, 10)(9, 11), (8, 10, 12)(9, 11, 13), (123)(567) diag$\{1^8\beta^6\}$.

(vii) M_{14} :

0 1 2 3	4 5 6 7	8 9 10 11	12 13
1 1 1 1 0	1 1 1 1	0 1 1 1 1	
0 0 1 1 0 1 0 1 0 0 0 0 0 0 0 0	0 0 1 1 0 1 0 1 0 1 0 1 0 0 1 1	0 0 1 1 0 0 0 0 0 1 0 1 0 0 β β	0 0 1 1 β β α β

[14, 7, 4], $A_4 = 9, g = 3 \cdot 3! \cdot 4^3 = 1152$, with generators (01)(23), (04)(16)(25)(37)(9, 10)(12, 13) diag$\{1^4\beta^4\alpha^4\beta 1\}$, (048)(159)(2, 6, 10)(3, 7, 11) diag$\{1^{12}\beta^2\}$.

Table continued

TABLE V (*Continued*)

(ix) N_{14} :

0	1	2	3	4	5	6	7	8	9	10	11	12	13
1	1	1	1										
				1	1	1	1						
		0						1	1	1	1	1	1
0	0	1	1	0	0	0	0	0	0	1	1	α	α
0	1	0	1	0	0	0	0	0	β	β	1	1	0
0	0	0	0	0	0	1	1	0	1	α	0	1	α
0	0	0	0	0	1	0	1	0	1	1	β	β	0

[14, 7, 4], $A_4 = 6$, $g = 3 \cdot 576 = 1728$, with generators
(01)(23), (04)(15)(26)(37)(9, 11)(10, 12), (123)(576)(9, 13, 11) diag$\{1^4\alpha^4\beta^6\}$,
(12)(67)(8, 11)(9, 12)(10, 13),

(x) Q_{14} : The [14, 7, 6] extended quadratic residue code defined in Table VI, with $A_4 = 0$ and $g = 3 \cdot |PSL_2(13)| = 3276$.

The monomial diag$\{\alpha\ \alpha \cdots \alpha\}$ has been omitted from the list of generators. We have usually not tried to give a minimal set of generators, as this would have obscured the structure of the group.

The codes in Table IV are all even and indecomposable. There are two infinite families: d_m ($m = 4, 6, 8,...$) and E_n ($n = 6, 8, 10,...$) (although some of the properties of E_6 and E_8 are different from those of the other E_n), and two codes e_5 and e_7 which belong to neither family.

THEOREM 29. *The only indecomposable even codes which are generated by code words of weight* 4 *are* d_m ($m = 4, 6, 8,...$), e_5, E_6, e_7, *and* E_8. *Hence if* $\mathscr{C}$ *is an even code with minimum distance* 4, *and* $\mathscr{D}$ *is the subcode of* $\mathscr{C}$ *generated by the words of weight* 4, *then* $\mathscr{D}$ *is a direct sum of codes equivalent to* d_m ($m = 4, 6, 8,...$), e_5, E_6, e_7, *or* E_8. *If* $\mathscr{D}$ *contains* E_6 *or* E_8, $\mathscr{C}$ *itself is decomposable.*

For example, if $\mathscr{C} = B_{10}$ (Table V) then $\mathscr{D} = e_5 \oplus e_5$. The codes d_m, e_5, E_6, e_7, E_8 are related by inclusion as shown in Fig. 1.

The last part of Theorem 29 also follows from:

THEOREM 30. *Any code word of* $d_m^{\perp}$ *is equivalent to one of* $\mathbf{0}, 00 \cdots 0011$, $1010 \cdots 1010$, *or* $1010 \cdots 10\alpha\beta$ (mod d_m). *Any code word of* $e_5^{\perp}$ *is equivalent to* $\mathbf{0}$ *or* $01\beta\alpha0$ (mod e_5). *Any code word of* $e_7^{\perp}$ *is equivalent to* $\mathbf{0}$ *or* $\mathbf{1}$ (mod e_7). *Finally any code word of* $E_6^{\perp}$ *or* $E_8^{\perp}$ *is equal to* $\mathbf{0}$ (mod E_6 *or* E_8, *respectively*).

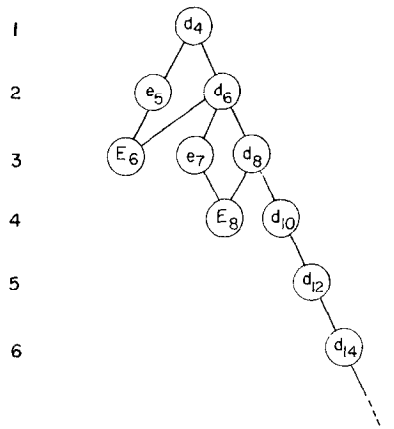


FIG. 1. Inclusion relations between indecomposable even codes generated by code words of weight 4.

The notation in Table V is the same as in Table IV. The weight enumerator of a code of length 12 in this table is given by $W = \eta_{12} + A_4\theta_6^2$, and that of a code of length 14 by $W = \eta_{14} + A_4\eta_2\theta_6^2$, where A_4 is the number of code words of weight 4.

We omit the proof of Theorem 27. Sufficient information about the groups is given in Table V to enable the reader to duplicate our calculations (compare also [30, proofs of Theorems 7.1 and 7.2]).

As a Corollary to Theorem 27 we can answer a question raised by Bassalygo *et al.* [5] in 1974. They discovered a set of possible parameters for a family of uniformly packed codes over $GF(4)$ (see also Goethals and van Tilborg [14]) and conjectured that codes exist with these parameters. In fact the first code in this family cannot be a linear code.

THEOREM 31. *There is no uniformly packed quasi-perfect linear code of length* 11 *over* $GF(4)$ *which is double-error-correcting and whose dual code has weights* 0, 6, 8, *and* 10.

Proof. Suppose $\mathscr{C}$ is such a code. Then $\mathscr{C}$ and $\mathscr{C}^\perp$ have parameters [11, 6, 5] and [11, 5, 6], respectively. Since $\mathscr{C}^\perp$ is even, by Theorem 1 $\mathscr{C} \supset \overline{\mathscr{C}}^\perp$, say $\mathscr{C} = \langle \overline{\mathscr{C}}^\perp, \mathbf{u} \rangle$ with $\mathrm{wt}(\mathbf{u}) = 5$. If G is a generator matrix for $\overline{\mathscr{C}}^\perp$, then

$$\left[\begin{array}{c|c} G & 0 \\ \hline \mathbf{u} & 1 \end{array}\right]$$

is the generator matrix for an even [12, 6, 6] code. But from Table V we see that no such code exists. Q.E.D.

OPEN PROBLEMS (continued). (5) Let $\mathscr{C}$ be an even f.s.d. code. Is $\mathscr{C}$ always monomially equivalent to $\bar{\mathscr{C}} = \mathscr{C}^{\perp}$? It is if $n \leqslant 14$ from Theorem 27 and Table V. Furthermore:

THEOREM 32. *If $\mathscr{C}$ is even f.s.d. and has a generator matrix of the form $[I \mid B]$ with B either symmetric or circulant then $\mathscr{C} \approx \bar{\mathscr{C}}$.*

Proof. (i) If B is symmetric then a generator matrix for $\bar{\mathscr{C}}$ is $B[I \mid \bar{B}] = [B \mid I]$ (from (2)), and this is clearly equivalent to $\mathscr{C}$. (ii) Left circulants are symmetric, and right circulants are equivalent to left circulants. Q.E.D.

(6) What is the weight distribution of E_n ?

5. EXTENDED CYCLIC CODES

In this section we study even f.s.d. codes over $GF(4)$ which are extended cyclic codes. Some examples are given in Table VI.

The reader is assumed to be familiar with the standard theory of cyclic codes (see [21]). If $\mathscr{C}$ is a cyclic code of length n with typical code word $(u_0 \cdots u_{n-1})$, the *extended* code $\mathscr{C}^*$ consists of the code words $(u_0 \cdots u_{n-1}u_\infty)$ with $u_\infty = \sum_{i=0}^{n-1} u_i$.

Since the extended code is to be f.s.d., we consider only odd n. A cyclotomic coset mod n has the form $C_s^{(4)} = \{s, 4s, 4^2s, \ldots, 4^{k(s)-1}s\}$, where $k(s)$ is the least integer such that $4^{k(s)} \equiv s \pmod{n}$. Let $\xi \in GF(4^{k(1)})$ be a primitive nth root of unity.

Quadratic residue codes are an important subclass of cyclic codes. Let p be an odd prime, and let R and N be, respectively, the quadratic residues and nonresidues mod p. Then R is a union of cyclotomic cosets $C_s^{(4)}$ mod p. The *quadratic residue* (or QR) code Q_p is the $[p, \frac{1}{2}(p+1)]$ cyclic code with generator polynomial $\prod_{i \in R}(x + \xi^i)$. Let $Q_{p+1} = Q_p^*$ denote the $[p+1, \frac{1}{2}(p+1)]$ extended QR code. It is easily verified that $Q_{p+1} \approx Q_{p+1}^{\perp}$; but as we see later Q_{p+1} need not be even. QR codes have been extensively studied by Assmus and Mattson [1–4], and we refer to [1] for the proof of the Gleason–Prange theorem that $\mathrm{Aut}(Q_{p+1})$ contains a subgroup isomorphic to $PSL_2(p)$ ($Q_6 \approx E_6$ is the only known case over $GF(4)$ in which the group is bigger than this).

DEFINITION. An odd positive integer n is called *feasible* if the set $\Omega = \{1, 2, \ldots, n-1\}$ can be partitioned into disjoint sets I, J such that (i) $2I \equiv -J \pmod{n}$ and (ii) I (and therefore J) is a union of cyclotomic cosets mod n. Otherwise n is *infeasible*.

TABLE VI

Cyclic Codes $\mathscr{C}$ for which $\mathscr{C}^*$ is Even f.s.d.

$n = 5$, $[6, 3, 4] = Q_6 \approx E_6$, and

$$E(x) = 1 + \alpha(x + x^4) + \beta(x^2 + x^3).$$

$n = 13$, $[14, 7, 6] = Q_{14}$, and

$$E(x) = 1 + \alpha(x + x^3 + x^4 + x^9 + x^{10} + x^{12}) + \beta(x^2 + x^5 + x^6 + x^7 + x^8 + x^{11}).$$

$n = 17$, $[18, 9, 8] = S_{18}$ with weight enumerator η_{18}, cyclotomic cosets are $\{1, 4, 16, 13\}$, $\{2, 8, 15, 9\}$, $\{3, 12, 14, 5\}$, $\{6, 7, 11, 10\}$, and

$$E(x) = 1 + \alpha\left(\sum_{i \in C_1^{(4)}} x^i + \sum_{i \in C_3^{(4)}} x^i\right) + \beta\left(\sum_{i \in C_2^{(4)}} x^i + \sum_{i \in C_6^{(4)}} x^i\right),$$

$n = 25$, $[26, 13, 4]$, cyclotomic cosets are $\{1, 4, 16, 14, 6, 24, 21, 9, 11, 19\}$, $\{2, 8, 7, 3, 12, 23, 17, 18, 22, 13\}$, $\{5, 20\}$, $\{10, 15\}$, and

$$E(x) = 1 + \alpha\left(\sum_{i \in C_1^{(4)}} x^i + \sum_{i \in C_5^{(4)}} x^i\right) + \beta\left(\sum_{i \in C_2^{(4)}} x^i + \sum_{i \in C_{10}^{(4)}} x^i\right).$$

$n = 29$, $[30, 15, 12] = Q_{30}$ with weight enumerator η_{30}, two cyclotomic cosets $R = C_1^{(4)}$ and $N = C_2^{(4)}$ each containing 14 elements, and

$$E(x) = 1 + \alpha \sum_{i \in R} x^i + \beta \sum_{i \in N} x^i.$$

THEOREM 33. *If n is feasible and $\Omega = I \cup J$ is the partition specified by the definition, then the cyclic code of length n with zeros $\{\xi^i : i \in I\}$ can be extended to an even f.s.d. code. Conversely, if there exists an even f.s.d. of length $n + 1$ which is an extended cyclic code then n is feasible.*

Proof. Let $\mathscr{C}$ be an $[n, \frac{1}{2}(n + 1)]$ cyclic code such that $\mathscr{C}^*$ is an even f.s.d. code. Suppose the zeros of $\mathscr{C}$ are $\{\xi^i : i \in I\}$. Note that $0 \notin I$, or else $\mathscr{C}^*$ would have a zero coordinate, contradicting Corollary 3. Let $J = \Omega - I$. Then $\overline{\mathscr{C}}$ has zeros $\{\xi^{2i} : i \in I\}$ and $\mathscr{C}^\perp$ has zeros $\{\xi^{-j} : j \in J \cup \{0\}\}$. From Theorem 4, $\overline{(\mathscr{C}^*)} = (\mathscr{C}^*)^\perp$. Now $\overline{(\mathscr{C}^*)}$ is the extension of $\overline{\mathscr{C}}$, and $(\mathscr{C}^*)^\perp$ is generated by $\mathbf{1}$ and $\{|\,\mathbf{u}\,|\,0\,| : \mathbf{u} \in \mathscr{C}^\perp\}$. Therefore $\overline{\mathscr{C}} = \langle \mathscr{C}^\perp, \mathbf{1} \rangle$ which implies $2I \subseteq -J \cup \{0\}$, hence $2I = -J$. The converse follows by reversing the argument. Q.E.D.

COROLLARY 34. *n is feasible if and only if $C_s^{(4)} \neq -2C_s^{(4)}$ for all s with $1 \leqslant s \leqslant n-1$.*

Proof (If). Put $C_s^{(4)}$ in I and $-2C_s^{(4)}$ in J. Q.E.D.

For example, $n = 5$ is feasible: we take $I = C_1^{(4)} = \{1, 4\}$, $J = C_2^{(4)} = \{2, 3\}$, $\eta \in GF(4^2)$, obtaining the QR code Q_5 with generator polynomial $(x + \eta)(x + \eta^4) = x^2 + \beta x + 1$. The extended code Q_6 has generator matrix

$$\begin{bmatrix} 1 & \beta & 1 & 0 & 0 & \beta \\ 0 & 1 & \beta & 1 & 0 & \beta \\ 0 & 0 & 1 & \beta & 1 & \beta \end{bmatrix}, \tag{31}$$

and is equivalent to E_6 of Table IV.

The numbers 5, 7, 13, 17, 23, 25, 29,... are feasible and 3, 9, 11, 15, 19, 21, 27,... are infeasible. We proceed to find some other tests for feasibility.

THEOREM 35. *n is feasible if and only if n and $2^{2i-1} + 1$ are relatively prime for all $i = 1, 2, \ldots$.*

Proof. If n is infeasible, then by Corollary 34, $2s \equiv -4^i s \pmod{n}$ for some s, i. This implies that n and $2^{2i-1} + 1$ have a common factor. Similarly for the converse. Q.E.D.

COROLLARY 36. *A product of feasible numbers is feasible. A number with an infeasible factor is infeasible.*

THEOREM 37. *Primes of the form $8m - 1$ and $8m - 3$ are feasible, primes of the form $8m + 3$ are infeasible, and primes of the form $8m + 1$ may or may not be feasible.*

Proof. Let e be the smallest positive integer such that $2^e \equiv 1 \pmod{p}$. Theorem 35 implies that p is feasible if $e \equiv 0, 1$, or $3 \pmod 4$, and is infeasible if $e \equiv 2 \pmod 4$. Suppose g is a primitive element of $GF(p)$ and $2 = g^t$ in $GF(p)$. Then

$$e = \frac{p-1}{\mathrm{GCD}\{p-1, t\}}. \tag{32}$$

If $p = 8m - 1$, then 2 is a quadratic residue mod p, t is even, $e = (4m - 1)/\mathrm{GCD}\{4m - 1, t/2\}$ is odd, and so p is feasible. Similarly for the other cases. The examples $p = 17$ and 281 show that an $8m + 1$ prime may or may not be feasible. Q.E.D.

THEOREM 38. *Suppose n is a product of primes of the form $8m - 1$. Then the extended cyclic code $\mathscr{C}^*$ of length $n + 1$ has a binary generator matrix*

and is strictly self-dual. $\mathscr{C}$ itself has a binary generator polynomial and idempotent.

This is an immediate consequence of:

LEMMA 39. *If n is a product of primes of the form $8m - 1$, then each cyclotomic coset $C_s^{(4)}$ coincides with $C_s^{(2)} = \{s, 2s, 2^2s, \ldots\} \bmod n$, and $2C_s^{(4)} = C_s^{(4)}$.*

Proof. It suffices to prove that $2 \in C_1^{(4)}$, and this holds if there is an odd number e with $2^e \equiv 1 \pmod n$. Suppose $n = \prod p_i^{a_i}$, p_i prime. We show that there exist odd numbers e_i with $2^{e_i} \equiv 1 \pmod{p_i^{a_i}}$. This implies that $e = lcm\{e_i\}$ is odd and satisfies $2^e \equiv 1 \pmod n$. Now 2 is a quadratic residue mod p_i, and therefore is a quadratic residue mod $p_i^{a_i}$ since p_i is odd. Let g be a primitive element of $GF(p_i^{a_i})$ and $2 = g^{2t}$. Then

$$e_i = \frac{\phi(p_i^{a_i})}{\mathrm{GCD}\{\phi(p_i^{a_i}), 2t\}} = \frac{p_i^{a_i - 1}(p_i - 1)/2}{\mathrm{GCD}\{p_i^{a_i - 1}(p_i - 1)/2, t\}} \tag{33}$$

is odd. Q.E.D.

Similar arguments establish Theorems 40–42.

THEOREM 40. *Suppose n is a product of primes p_i of the form $8m + 1$ such that, for suitable t_i, $2^{4t_i+1} \equiv 1 \pmod{p_i}$. Then the conclusions of Theorem 38 hold.*

Examples of such primes are 73 and 89. Of course Theorems 38 and 40 deal with the least interesting case, when the codes are the $GF(4)$ spans of binary codes.

THEOREM 41. *Suppose n is a product of primes of the form $8m - 3$. Then $-1 \in C_1^{(4)}$, $2 \notin C_1^{(4)}$, and $\mathscr{C}$, $\mathscr{C}^*$ do not have binary bases.*

THEOREM 42. *Suppose n is a prime of the form $8m + 1$ such that, for some t, $2^{4t} \equiv 1 \pmod p$. Then the conclusions of Theorem 41 hold.*

It is often easier to find the idempotent

$$E(x) = \sum_s \epsilon_s \sum_{i \in C_s} x^i \tag{34}$$

of a cyclic code than the generator polynomial. The outer summation in (34) is over all distinct cyclotomic cosets, including $s = 0$. The coefficients ϵ_s must satisfy the following constraints, which make it simple to guess $E(x)$. If $C_s^{(4)} = C_{2s}^{(4)}$ then $\epsilon_s = 0$ or 1. If $C_s^{(4)} \neq C_{2s}^{(4)}$ then $(\epsilon_s, \epsilon_{2s}) = (\alpha, \beta), (\beta, \alpha)$,

or (0, 0). If r and s are both in I or both in J then $E(\xi^r) = E(\xi^s)$. If $r \in I$, $s \in J$ then $E(\xi^r) + E(\xi^s) = 1$. The constant term ϵ_0 is determined by $E(1) = 1$.

For example, if $p = 8m - 3$ we take $I = R$, $J = N$ and obtain the QR code Q_p with idempotent

$$E(x) = 1 + \alpha \sum_{i \in R} x^i + \beta \sum_{i \in N} x^i. \tag{35}$$

The extended code Q_{p+1} is even f.s.d. If $p = 8m - 1$, Q_p has idempotent

$$E(x) = \sum_{i \in R} x^i, \tag{36}$$

and Q_{p+1} is even and strictly self-dual. If $p = 8m + 3$, Q_{p+1} is not even by Theorem 37.

Table VI shows examples of extended cyclic codes which are even f.s.d. and which do not have a binary basis, for all lengths $n + 1 \leqslant 34$. The table gives n, the parameters $[n + 1, \frac{1}{2}(n + 1), d]$ of the extended code, the cyclotomic cosets $C_s^{(4)} \bmod n$ (in some cases), and the idempotent of the cyclic code.

Remarks. (1) The minimum weight of S_{18} was determined by computer.

(2) By shortening S_{18} we found a [16, 8, 6] even f.s.d. code R_{16}, with generator matrix $[I \mid B]$, where

$$B = \begin{bmatrix} 0 & 0 & \alpha & 1 & 1 & 1 & 0 & \beta \\ 1 & \beta & \alpha & \beta & 1 & 1 & 0 & 1 \\ \beta & \beta & \beta & \alpha & 0 & \alpha & \alpha & 1 \\ 1 & 0 & \alpha & 0 & 0 & \alpha & \beta & \alpha \\ 1 & \alpha & 0 & \alpha & 1 & 1 & \beta & 1 \\ \alpha & 0 & 1 & \alpha & \alpha & 1 & \beta & 1 \\ 1 & 1 & 1 & \alpha & 0 & 0 & 0 & \beta \\ \beta & \beta & \alpha & \beta & \beta & 1 & \beta & 0 \end{bmatrix}.$$

(3) The minimum weight of Q_{30} was given by Assmus and Mattson in [2]. We verified this by computer.

6. Unitary Matrices

In view of Theorem 5 we can also find even f.s.d. codes by constructing matrices B over $GF(4)$ with $B\bar{B}^T = I$. Such matrices are called *unitary*. In this section we determine the number of circulant unitary matrices and show how to find them. The material in this section is similar to that in [18, 19] and only the differences are given in any detail.

Unitary matrices of order m form a subgroup $\mathscr{M}_m = GU(m, 2)$ of the general linear group $GL(m, 4)$ of all invertible $m \times m$ matrices over $GF(4)$. It is well known that the order of $\mathscr{M}_m$ is

$$|\mathscr{M}_m| = 2^{m(m-1)/2} \prod_{i=1}^{m} (2^i - (-1)^i) \tag{37}$$

(see for example [12, Theorem 115] or [13, p. 50]; compare also [18]).

Let $\mathscr{S}_m$ be the subgroup of $\mathscr{M}_m$ consisting of all right circulant $m \times m$ unitary matrices (cf. [19]).

THEOREM 43. (a) *If m is odd*

$$|\mathscr{S}_m| = \prod_s (2^{k(s)} + 1) \prod_t (4^{k(t)} - 1), \tag{38}$$

where every cyclotomic coset such that $C_s^{(4)} = -C_{-2s}^{(4)}$ (including $s = 0$) contributes one term to the first product, and every pair such that $C_s^{(4)} \neq -C_{-2t}^{(4)}$ contributes one term to the second product.

(b) *If $m = 2\mu$ then*

$$|\mathscr{S}_{2\mu}| = 2^{\mu} |\mathscr{S}_{\mu}|. \tag{39}$$

Proof. The proof also shows how to construct these circulants. We work in the ring $\mathscr{R}_m = GF(4)[x]/(x^m + 1)$. A circulant A with first row $a_0 a_1 \cdots a_{m-1}$ is specified by the element $a(x) = \sum_{i=0}^{m-1} a_i x^i$ of $\mathscr{R}_m$. Then $\bar{A}$ and A^T are represented by

$$\overline{a(x)} = \sum_{i=0}^{m-1} a_i^2 x^i, \tag{40}$$

$$a(x)^T = \sum_{i=0}^{m-1} a_i x^{m-i} = a_0 + \sum_{i=1}^{m-1} a_{m-i} x^i, \tag{41}$$

and $A\bar{A}^T = I$ if and only if $a(x)\,\overline{a(x)}^T = 1$ in $\mathscr{R}_m$.

Case (a), *m odd.* $\mathscr{R}_m$ is a semisimple group algebra over $GF(4)$, which is the direct sum of its minimal ideals

$$\mathscr{R}_m = \mathscr{I}_0 \oplus \mathscr{I}_1 \oplus \cdots \oplus \mathscr{I}_n.$$

Let ξ be a primitive mth root of unity over $GF(4)$. For each r there is a unique $s = s(r)$ such that the nonzeros of $\mathscr{I}_r$ are $\{\xi^i : i \in C_s^{(4)}\}$, where $C_s^{(4)}$ is a cyclotomic coset mod m. Then $\mathscr{I}_r$ has dimension $k(s)$ and is isomorphic to the field $GF(4^{k(s)})$. One such isomorphism is given by $a(x) \in \mathscr{I}_r \to a(\xi^s) \in GF(4^{k(s)})$.

We now show that the number of $b(x) \in \mathscr{R}_m$ with $b(x)\,\overline{b(x)}^T = 1$ is given by (38). Write such a $b(x)$ as $\sum_{r=0}^{m} b_r(x)$, $b_r(x) \in \mathscr{I}_r$. Since $b(x)$ is invertible in $\mathscr{R}_m$, $b_r(x) \neq 0$. Let $\mathscr{I}_0, \ldots, \mathscr{I}_l$ be the minimal ideals with $\mathscr{I} = \mathscr{I}^T$ (and $C_s^{(4)} = -C_{-2s}^{(4)}$), with $\mathscr{I}_0$ corresponding to $C_0^{(4)} = \{0\}$. Let the remaining ideals be numbered so that $\mathscr{I}_{l+1} = \mathscr{I}_{l+2}^T$, etc. Let $E_r(x)$ be the idempotent of $\mathscr{I}_r$. Suppose

$$b(x) = \sum_{s=0}^{l} a_s(x) + \sum_{t=l+1,\,l+3,\ldots} (c_t(x) + c_{t+1}(x)) \tag{42}$$

with $a_s(x) \in \mathscr{I}_s$, $c_t(x) \in \mathscr{I}_t$. Then

$$1 = \sum_{s=0}^{l} E_s(x) + \sum_{t=l+1,\,l+3,\ldots} (E_t(x) + E_{t+1}(x)),$$

$$1 = b(x)\,\overline{b(x)}^T = \sum_{s=0}^{l} a_s(x)\,\overline{a_s(x)}^T + \sum_{t=l+1,\,l+3,\ldots} (c_t(x)\,\overline{c_{t+1}(x)}^T + \overline{c_t(x)}^T c_{t+1}(x)), \tag{43}$$

$$a_s(x)\,\overline{a_s(x)}^T = E_s(x), \qquad c_t(x)\,\overline{c_{t+1}(x)}^T = E_t(x). \tag{44}$$

LEMMA 44. *There are* $4^{k(t)} - 1$ *ways of choosing* $c_t(x) + c_{t+1}(x)$ *in* (42).

Proof. $c_t(x)$ is any nonzero element of $\mathscr{I}_t$ and $c_{t+1}(x)$ is uniquely determined by (44). Q.E.D.

LEMMA 45. *There are* $2^{k(s)} + 1$ *ways of choosing* $a_s(x)$ *in* (42).

Proof. Let $k = k(s)$ and let $\theta \in GF(4^k)$ be a nonzero of $\mathscr{I}_s$. Then $a(x) \to a(\theta)$ is an isomorphism of $\mathscr{I}_s$ onto $GF(4^k)$. From (40) and (41), $\overline{a(x)}^T \to a(\theta^{-1/2})^2$.

The nonzeros of $\mathscr{I}_s$ are $\theta, \theta^4, \ldots, \theta^{4^{k-1}}$, and $4^k \equiv 1$, $2^k \equiv -1$, and $-\frac{1}{2} \equiv 4^{(k-1)/2} \pmod m$. Since $\mathscr{I}_s = \mathscr{I}_s^T$, $-2 \equiv 4^i \pmod m$ for some i, thus $2^{2i-1} \equiv -1 \pmod m$. Therefore $k = 2i - 1$ is odd, and $\theta^{-1/2} = \theta^{4(k-1)/2}$.

Then $a(x)\,\overline{a(x)}^T = E(x)$ implies $a(\theta)^{2^k+1} = 1$ in $GF(4^k)$. Every zero of $z^{2^k+1} - 1$ is in $GF(4^k)$, so there are $2^k + 1$ choices for $a(x)$. Q.E.D.

This completes the proof of Theorem 43(a). As an example we find all 5×5 unitary circulants B. Thus $m = 5$, $C_0^{(4)} = \{0\}$, $C_1^{(4)} = \{1, 4\}$, $C_2^{(4)} = \{2, 3\}$, $\mathscr{I}_0 = \mathscr{I}_0^T$, $\mathscr{I}_1 = \mathscr{I}_2^T$, $E_0(x) = 1 + x + \cdots + x^4$, $E_1(x) = 1 + \alpha x + \beta x^2 + \beta x^3 + \alpha x^4$. Then $c_1(x) = \alpha + x + \alpha x^2 + \beta x^3 + \beta x^4 \in \mathscr{I}_1$, and $c_2(x) = \beta + x + \beta x^2 + \alpha x^3 + \alpha x^4 \in \mathscr{I}_2$ satisfies $c_1(x)\,\overline{c_2(x)}^T = E_1(x)$. Thus $b(x) = E_0(x) + c_1(x) + c_2(x) = x$ is a circulant. In this way we find that the first row

of B is a cyclic permutation or scalar multiple of 10000, $1\alpha\alpha\alpha\alpha$, or $1\beta\beta\beta\beta$, and $|\mathscr{S}_5| = 45$.

Case (b), $m = 2\mu$. $\mathscr{R}_m$ is no longer semisimple. Let $\mathscr{I}_\mu$ be the ideal of $\mathscr{R}_m$ generated by $x^\mu + 1$, with $\mathscr{I}_\mu = \mathscr{I}_\mu^{T}$, $|\mathscr{I}_\mu| = 4^\mu$. Each coset of $\mathscr{I}_\mu$ in $\mathscr{R}_m$ contains exactly one element of degree $<\mu$, say $u(x)$, which may be regarded as an element of $\mathscr{R}_\mu$. Changing notation slightly, let T_μ denote the transpose in $\mathscr{R}_\mu$ and T_m the transpose in $\mathscr{R}_m$. The idea of the proof is to show that for each circulant in $\mathscr{S}_\mu$ there 2^μ circulants in $\mathscr{S}_m$.

The first step is to show that if $b(x) \in \mathscr{R}_m$ satisfies $b(x)\,b(x)^{T_m} = 1$ and is in the coset $u(x) + \mathscr{I}_\mu$ then

$$u(x)\,\overline{u(x)^{T_\mu}} = 1, \tag{45}$$

$$u(x)\,\overline{u(x)^{T_m}} = 1 + r(x) + \overline{r(x)^{T_m}} \tag{46}$$

for some $r(x) \in \mathscr{I}_\mu$, and

$$b(x) = u(x) + r(x)(\overline{u(x)^{T_m}})^{-1}. \tag{47}$$

Conversely, given $u(x) \in \mathscr{R}_\mu$ satisfying (45), there are 2^μ of the $r(x)$ satisfying (46) and therefore 2^μ $b(x)$ given by (47). We omit the straightforward details (compare [19]).

Note added in proof. For a sequel to this paper see J. H. Conway, V. Pless, and N. J. A. Sloane, Self-dual codes over $GF(3)$ and $GF(4)$ of length not exceeding 16, *IEEE Trans. Inform. Theory*, **IT-25** (1979), to appear.

ACKNOWLEDGMENTS

We should like to thank J. M. Goethals for telling us about the question answered by Theorem 32, and S. I. Feldman for writing a computer program to verify the minimum weight of Q_{30} (see Section 5). We also thank J. MacKay and C. C. Sims for computing the orders of some permutation groups for us, and especially V. Pless, who made it possible for us to use her CAMAC (Combinatorial and Algebraic Machine Aided Computation) system [29]. We also made use of the ALTRAN [8, 15] and UNIX [31, 34] systems at Bell Labs and the MACSYMA system [27] at MIT.

REFERENCES

1. E. F. ASSMUS, JR., AND H. F. MATTSON, JR., New 5-designs, *J. Combinatorial Theory* **6** (1969), 122–151.
2. E. F. ASSMUS, JR., AND H. F. MATTSON, JR., On weights in quadratic-residue codes, *Discrete Math.* **3** (1972), 1–20.

3. E. F. ASSMUS, JR., AND H. F. MATTSON, JR., Coding and combinatorics, *SIAM Rev.* **16** (1974), 349–388.
4. E. F. ASSMUS, JR., H. F. MATTSON, JR., AND R. J. TURYN, Research to develop the algebraic theory of codes, Report AFCRL-67-0365, Air Force Cambridge Res. Labs., Bedford, Mass., June 1967.
5. L. A. BASSALYGO, G. V. ZAITSEV, AND V. A. ZINOVIEV, Uniformly packed codes, *Problems of Information Transmission* **10** (No. 1, 1974), 6–9.
6. M. BROUÉ, Codes correcteurs d'erreurs auto-orthogonaux sur le corps à deux éléments et formes quadratiques entières définies positives à discriminant $+1$, *in* "Comptes Rendus des Journées Mathématiques de la Société Math. de France," pp. 71–108, Univ. Sci. Tech. Languedoc, Montpellier, 1974. Also *Discrete Math.* **17** (1977), 247–269.
7. M. BROUÉ AND M. ENGUEHARD, Polynômes des poids de certains codes et fonctions thêta de certains réseaux, *Ann. Sci. École Norm. Sup.* **5** (1972), 157–181.
8. W. S. BROWN, "ALTRAN User's Manual," 3rd ed., Bell Laboratories, Murray Hill, N.J., 1974.
9. J. H. CONWAY, Groups, lattices, and quadratic forms, *in* "Computers in Algebra and Number Theory," pp. 135–139, SIAM–AMS Proc., Vol. IV, Amer. Math. Soc., Providence, R.I., 1971.
10. J. H. CONWAY AND V. PLESS, On the enumeration of self-dual codes, *J. Combinatorial Theory*, to appear.
11. H. S. M. COXETER AND W. O. J. MOSER, "Generators and Relations for Discrete Groups," 2nd ed., Springer-Verlag, New York, 1965.
11a. P. DEMBOWSKI, "Finite Geometries," Springer-Verlag, New York, 1968.
12. L. E. DICKSON, "Linear Groups with an Exposition of the Galois Field Theory," Dover, New York, 1958.
13. J. A. DIEUDONNÉ, "La géométrie des groupes classiques," 3rd ed., Springer-Verlag, New York 1971.
14. J.-M. GOETHALS AND H. C. A. VAN TILBORG, Uniformly packed codes, *Philips Res. Rep.*, **30** (1975), 9–36.
15. A. D. HALL, JR., The ALTRAN system for rational function manipulation—a survey, *Comm. ACM* **14** (1971), 517–521.
16. W. C. HUFFMAN, Polynomial invariants of finite linear groups of degree two, preprint.
17. F. J. MACWILLIAMS, A theorem on the distribution of weights in a systematic code, *Bell Syst. Tech. J.* **42** (1963), 79–94.
18. F. J. MACWILLIAMS, Orthogonal matrices over finite fields, *Amer. Math. Monthly* **76** (1969), 152–164.
19. F. J. MACWILLIAMS, Orthogonal circulant matrices over finite fields, and how to find them, *J. Combinatorial Theory* **10** (1971), 1–17.
20. F. J. MACWILLIAMS, C. L. MALLOWS, AND N. J. A. SLOANE, Generalizations of Gleason's theorem on weight enumerators of self-dual codes, *IEEE Trans. Information Theory* **18** (1972), 794–805.
21. F. J. MACWILLIAMS AND N. J. A. SLOANE, "The Theory of Error-Correcting Codes," North–Holland, Amsterdam, 1977.
22. F. J. MACWILLIAMS, N. J. A. SLOANE, AND J. G. THOMPSON, Good self-dual codes exist, *Discrete Math.* **3** (1972), 153–162.
23. F. J. MACWILLIAMS, N. J. A. SLOANE, AND J. G. THOMPSON, On the existence of a projective plane of order 10, *J. Combinatorial Theory, Ser. A* **14** (1973), 66–78.
24. C. L. MALLOWS, A. M. ODLYZKO, AND N. J. A. SLOANE, Upper bounds for modular forms, lattices, and codes, *J. Algebra* **36** (1975), 68–76.
25. C. L. MALLOWS, V. PLESS, AND N. J. A. SLOANE, Self-dual codes over $GF(3)$, *SIAM J. Appl. Math.* **31** (1976), 649–666.

26. C. L. MALLOWS AND N. J. A. SLOANE, An upper bound for self-dual codes, *Inform. Contr.* **22** (1973), 188–200.
27. Mathlab Group, "MACSYMA Reference Manual," Version 8, Project MAC, MIT, Cambridge, Mass., 1975.
28. V. PLESS, A classification of self-orthogonal codes over $GF(2)$, *Discrete Math.* **3** (1972), 209–246.
29. V. PLESS, CAMAC, pp. 171-176 *in* "Proc. 1976 ACM Symposium on Symbolic and Algebraic Computation" (R. D. Jenks, ed.), Assoc. Comput. Mach., New York, 1976.
30. V. PLESS AND N. J. A. SLOANE, On the classification and enumeration of self-dual codes, *J. Combinational Theory, Ser. A* **18** (1975), 313–335.
31. D. M. RITCHIE AND K. THOMPSON, The UNIX time-sharing system, *Comm. ACM* **17** (1974), 365–375.
32. N. J. A. SLOANE, Weight enumerators of codes, *in* "Combinatorics" (M. Hall, Jr., and J. H. van Lint, Eds.), pp. 115–142, Reidel, Boston, and Math. Centre, Amsterdam, 1975.
33. N. J. A. SLOANE, Error-correcting codes and invariant theory: New applications of a nineteenth century technique, *Amer. Math. Monthly* **84** (1977), 82–107.
34. K. THOMPSON AND D. M. RITCHIE, "UNIX Programmer's Manual," 6th ed., Bell Laboratories, Murray Hill, N.J., 1976.
35. H. N. WARD, A restriction on the weight enumerator of a self-dual code, *J. Combinatorial Theory, Ser. A* **21** (1976), 253–255.
36. N. J. A. SLOANE, Self-dual codes and lattices, Proceedings of Symposia on Pure Maths., "Relations Between Combinatorics and Other Parts of Mathematics," Amer. Math. Soc., Providence, R.I., 1979, to appear.